Troubleshooting Tools

An overview of the main tools for verifying network operation from a host

Fulvio Risso
Mario Baldi
Politecnico di Torino
(Technical University of Turin)

© see page 2

Notes

- The commands/programs described in this presentation are commonly available both on UNIX and Windows workstations
- Nevertheless
  - Options and parameters might be different
  - Output might be different
- Hence …
  - Content of this presentation should not be taken literally
  - It should be used as a starting point
  - Command syntax and output should be double-checked
- Moreover only options and parameters considered relevant to our purposes are listed here
- For some commands an equivalent program with graphic interface might exist

ping

- Checks network reachability of a host
- Syntax:

```
ping [options] target
```

Option	Description
`-t`	ICMP Echo Request messages sent continually until Ctrl+C is pressed (in UNIX this is default behaviour).
`-c count`	Sends `count` ICMP Echo Request messages (in Windows default `count` is 4).
`-i TTL`	ICMP Echo Request messages are sent into IP packet with Time To Live field containing `TTL` (only Windows).
`-w timeout`	A reply is waited for at most `timeout` milliseconds; if a later reply is ignored.
`-R`	(Possibly) records path taken by packets by activating *Record Route* option in the ICMP Echo Request message.

ping Output Example

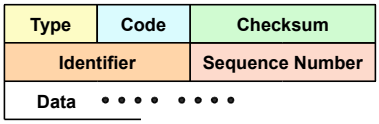
```
PING www.xenia.it (209.238.252.133): 56 data bytes
64 bytes from 209.238.252.133: icmp_seq=0 ttl=113 time=1318 ms
64 bytes from 209.238.252.133: icmp_seq=1 ttl=113 time=1738 ms
64 bytes from 209.238.252.133: icmp_seq=2 ttl=113 time=1756 ms
64 bytes from 209.238.252.133: icmp_seq=3 ttl=113 time=1808 ms
64 bytes from 209.238.252.133: icmp_seq=4 ttl=113 time=1804 ms
64 bytes from 209.238.252.133: icmp_seq=5 ttl=113 time=1751 ms
64 bytes from 209.238.252.133: icmp_seq=6 ttl=113 time=1617 ms
64 bytes from 209.238.252.133: icmp_seq=7 ttl=113 time=1526 ms
64 bytes from 209.238.252.133: icmp_seq=8 ttl=113 time=902 ms
64 bytes from 209.238.252.133: icmp_seq=9 ttl=113 time=1409 ms

----www.xenia.it PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 902/1562/1808 ms
```

Round-trip time (RTT): time elapsed from the transmission of an ICMP Echo Request to the reception of the corresponding ICMP Echo Reply; it is a measure of the "*distance*" between local and target host.

ping Working Principle

- Testing host sends an `ICMP Echo Request` message to target host
- Target host replies with `ICMP Echo Reply` message

0 = Echo Request
8 = Echo Reply



Interpreting ping Outcome

- If replies are received, connectivity to target host exists
- When replies are not received
  - A routing problem might exist on the path from local host to target
  - A routing problem might exist on path from target to local host
    - The two paths might not be the same
  - Routers might be configured not to forward IP packets containing ICMP messages
  - A firewall on the path might filter out ICMP messages
  - A Personal Firewall on the local host or target host might filter out ICMP messages

Traceroute

- Shows the (likely) path (or route) to the target host
  - Shows routers traversed by packets traveling from local host to target host
  - IP address or domain name of one interface of each router is shown
    - Not necessary the interface having received or forwarded the packet
- Syntax

```
traceroute [options] target (UNIX)
tracert [options] target (Windows)
```


Traceroute Output Example

```
traceroute to library.airnews.net (206.66.12.202), 30 hops max, 40 byte packets
 1  rbrt3 (208.225.64.50)  4.867 ms  4.893 ms  3.449 ms
 2  519.Hssi2-0-0.GW1.EWR1.ALTER.NET (157.130.0.17)  6.918 ms  8.721 ms  16.476 ms
 3  113.ATM3-0.XR2.EWR1.ALTER.NET (146.188.176.38)  6.323 ms  6.123 ms  7.011 ms
 4  192.ATM2-0.TR2.EWR1.ALTER.NET (146.188.176.82)  6.955 ms  15.400 ms  6.684 ms
 5  105.ATM6-0.TR2.DFW4.ALTER.NET (146.188.136.245)  49.105 ms  49.921 ms  47.371 ms
 6  298.ATM7-0.XR2.DFW4.ALTER.NET (146.188.240.77)  48.162 ms  48.052 ms  47.565 ms
 7  194.ATM9-0-0.GW1.DFW1.ALTER.NET (146.188.240.45)  47.886 ms  47.380 ms  50.690 ms
 8  iadfw3-gw.customer.ALTER.NET (137.39.138.74)  69.127 ms  68.112 ms  66.859 ms
 9  library.airnews.net (206.66.12.202)  174.853 ms  163.945 ms  147.501 ms
```

Round-trip time (RTT): time elapsed from the transmission of an ICMP Echo Request to the reception of the corresponding ICMP Time Exceedded message; it provides a very loose measure of the travel time between local host and each router.
Sometimes travel time changes significantly in the course of a few seconds due to temporary congestion of routers.

Traceroute Working Principle

1. Local host sends an `ICMP Echo Request` message in IP packet with TTL = 1
2. First router (default gateway) decrements TTL and discards IP packet and reacts sending `ICMP TTL Exceeded in Transit`
3. Local host receives `ICMP TTL Exceeded in Transit` and from source address of encapsulating IP packet learns one IP address of first router
   - Specific interface depends on router implementation
   - Might be interface through which IP packet was sent
4. Local host sends another `ICMP Echo Request` message in IP packet with incremented TTL (TTL = 2)
5. Default gateway forwards IP packet decrementing TTL (=1)
6. Second router on the path decrements TTL and discards IP packet and reacts sending `ICMP TTL Exceeded in Transit`

   Some Unix implementations send a UDP message rathern than an ICMP Echo Request message

Traceroute Options

Option	Description
`-f TTL`	`TTL` used as initial value for Time To Live field in first IP packet rather than the default 1.
`-I`	Uses ICMP Echo Request messages rather than UDP messaged (UNIX only).
`-p port`	Generates UDP messages to `port` destination port rather than default 33434 (UNIX only).
`-m count`	Uses `count` as the maximum value for the Time To Live field rather than the default 30.
`-w timeout`	A reply is waited for at most `timeout` milliseconds; if a later reply is ignored.
`-q count`	`count` test messages are generated for each value of the Time To Live field (default is three).

arp

- **Shows and modifies ARP cache content**
- **Syntax**

```
arp [options] [IPAddr] [EthAddr]
```

Options	Description
`-a`	Shows the current ARP cache content highlighting static and dynamic entries.
`-d IPAddr`	Eliminates from ARP cache MAC address mapping corresponding to host `IPAddr`.
`-s IPAddr EthAddr`	Adds stating mapping between network address `IPAddr` and data-link address `EthAddr`.

arp Sample Output

```
C:\>arp -a

Interface: 130.192.16.81 --- 0x30004
  Internet Address      Physical Address      Type
  130.192.16.17         00-e0-63-13-7e-01     dynamic
  130.192.16.36         00-10-4b-35-f2-fa     dynamic
```

netstat

- Shows main network parameters
- Syntax:

```
netstat [options]
```

Opzione	Descrizione
[no param.]	Lists active layer 4 connections and sessions.
-a	Lists active layer 4 connections and sessions, as well as TCP or UDP servers on the loacl host.
-s	Shows per-protocol (layer 3 and 4) statistics.
-e	Shows Ethernet card statistics.
-r	Displays IP routing table.

netstat Output Example

```
C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    truciolo:http          truciolo:0             LISTENING
  TCP    truciolo:epmap         truciolo:0             LISTENING
  TCP    truciolo:https         truciolo:0             LISTENING
  TCP    truciolo:2747          truciolo:0             LISTENING
  TCP    truciolo:2747          localhost:2748         ESTABLISHED
  TCP    truciolo:2748          localhost:2747         ESTABLISHED
  UDP    truciolo:microsoft-ds  *:*
  UDP    truciolo:isakmp        *:*
  UDP    truciolo:1030          *:*
  UDP    truciolo:1078          *:*
  UDP    truciolo:2040          *:*
  UDP    truciolo:2359          *:*
  UDP    truciolo:3456          *:*
  UDP    truciolo:4500          *:*
  UDP    truciolo:ntp           *:*
```


netstat Output Example

```
C:\>netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 10 4b 35 f2 fa ...... 3Com EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     130.192.3.17    130.192.28.4       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      130.192.0.0      255.255.0.0     130.192.28.4    130.192.28.4       1
     130.192.28.4  255.255.255.255        127.0.0.1       127.0.0.1       1
  130.192.255.255  255.255.255.255     130.192.28.4    130.192.28.4       1
        224.0.0.0        224.0.0.0     130.192.28.4    130.192.28.4       1
  255.255.255.255  255.255.255.255     130.192.28.4    130.192.28.4       1
Default Gateway:      130.192.3.17
===========================================================================
Persistent Routes:
  None
```

netstat Output Example

```
C:\>netstat -s

IPv4 Statistics
  Packets Received                    = 1762191
  Received Header Errors              = 12
  Received Address Errors             = 655093
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
  Received Packets Delivered          = 1127699
  Output Requests                     = 951452
  Routing Discards                    = 0
  Discarded Output Packets            = 0
  Output Packet No Route              = 8
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0

[continue ...]
```

```
[...continue]

ICMPv4 Statistics

                            Received    Sent
  Messages                  1246        1780
  Errors                    0           0
  Destination Unreachable   371         476
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echos                     555         749
  Echo Replies              168         555
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics for IPv4
  Active Opens                        = 8767
  Passive Opens                       = 769
  Failed Connection Attempts          = 420
  Reset Connections                   = 1436
  Current Connections                 = 3
  Segments Received                   = 759943
  Segments Sent                       = 768276
  Segments Retransmitted              = 1003
```


netstat Output Example

```
C:\>netstat -e

Interface Statistics

                           Received            Sent

Bytes                     458905257       313090297
Unicast packets              786574          805622
Non-unicast packets         1565173           34366
Discards                          0               0
Errors                            0             112
Unknown protocols            232253               0
```


route

- Displays and modifies IP routing table
- Syntax:

```
route [options] [command] [parameters]
```

Option	Description
`print`	Displays routing table; equivalent to `netstat -r`.
`add NetAddr mask NetMask Gateway`	Adds route for network `NetAddr/NetMask` (e.g., 10.0.0.0/255.255.255.0) through next hop `Gateway`.
`delete NetAddr mask NetMask Gateway`	Removes route for network `NetAddr/NetMask` (e.g., 10.0.0.0/255.255.255.0) through next hop `Gateway`.

ipconfig

- **Displays and modifies some of the IP stack parameters**
- **Syntax:**

```
ipconfig [options]
```

Option	Description
`[no param.]`	Displays main TCP/IP configuration data (addresses, netmask, default gateway, DNS server).
`/all`	Displays all TCP/IP configuration data (addresses, netmask, default gateway, DNS server, lease time for DHCP assigned addresses).
`/displaydns`	Displays local host DNS cache.
`/flushdns`	Flushes local host DNS cache.

ipconfig Output Example

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 130.192.16.81
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:760:400:1:3c71:db18:e713:fd56
        IP Address. . . . . . . . . . . . : 2001:760:400:1:20b:dbff:fe14:50bb
        IP Address. . . . . . . . . . . . : fe80::20b:dbff:fe14:50bb%8
        Default Gateway . . . . . . . . . : 130.192.16.17
                                            fe80::207:ebff:fe7e:c60%8
```


ipconfig Output Example

```
C:\>ipconfig /all

Windows IP Configuration
        Host Name . . . . . . . . . . . . : truciolo
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com 3C920 Fast Ethernet (3C905C-TX)
        Physical Address. . . . . . . . . : 00-0B-DB-14-50-BB
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 130.192.16.81
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:760:400:1:3c71:db18:e713:fd56
        IP Address. . . . . . . . . . . . : 2001:760:400:1:20b:dbff:fe14:50bb
        IP Address. . . . . . . . . . . . : fe80::20b:dbff:fe14:50bb%8
        Default Gateway . . . . . . . . . : 130.192.16.17
                                            fe80::207:ebff:fe7e:c60%8
        DNS Servers . . . . . . . . . . . : 130.192.3.21
                                            130.192.3.24
                                            fec0:0:0:ffff::1%1
                                            fec0:0:0:ffff::2%1
                                            fec0:0:0:ffff::3%1
```

ipconfig Output Example

```
C:\>ipconfig /displaydns

Windows IP Configuration

        www.polito.it
        ----------------------------------------
        Record Name . . . . . : www.polito.it
        Record Type . . . . . : 5
        Time To Live  . . . . : 86398
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        CNAME Record  . . . . : web01.polito.it

        localhost
        ----------------------------------------
        Record Name . . . . . : localhost
        Record Type . . . . . : 1
        Time To Live  . . . . : 0
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        A (Host) Record . . . : 127.0.0.1

        . . .
```